

# EXHIBIT 6

ebay

— PEOPLE WANT —  
**WHAT YOU GOT**

**SELL FOR THE MOST MONEY**



Apple iPhone 6  
16GB - Space Gray

**SOLD FOR**  
eBay **\$410**  
AT&T **\$300**

**Sell yours**

SHARE

SHARE  
806

TWEET  
1012

PIN

COMMENT  
21

EMAIL

ANDY GREENBERG SECURITY 09.10.15 7:00 AM

# GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS



An attendee demonstrates the OnStar dash system on a Chevrolet Impala during the 2014 North American International Auto Show. DANIEL ACKER/BLOOMBERG/GETTY IMAGES

WHEN A PAIR of security researchers showed they could hack a Jeep over the Internet earlier this summer to hijack its brakes and transmission, the impact was swift and explosive: Chrysler issued a software fix before the research was even made public. The National Highway Traffic and Safety Administration launched an investigation. Within



## LATEST NEWS



GADGET LAB PODCAST  
Gadget Lab Podcast: Test Mode  
34 MINS



MOVIES  
Here Is Your WIRED *Star Wars* Challenge for Day 145  
4 HOURS

days Chrysler issued a 1.4 million vehicle recall.



But when another group of researchers quietly pulled off that same automotive magic trick five years earlier, their work was answered with exactly none of those reactions. That's in part because the prior group of car hackers, researchers at the University of California at San Diego and the University of Washington, chose not to publicly name the make and model of the vehicle they tested, which has since been revealed to be General Motors' 2009 Chevy Impala. They also discreetly shared their exploit code only with GM itself rather than publish it.

The result, WIRED has learned, is that GM took nearly five years to fully protect its vehicles from the hacking technique, which the researchers privately disclosed to the auto giant and to the National Highway Traffic Safety Administration in the spring of 2010. For nearly half a decade, millions of GM cars and trucks were vulnerable to that privately known attack, a remote exploit that targeted its OnStar dashboard computer and was capable of everything from tracking vehicles to engaging their brakes at high speed to disabling brakes altogether.

---

**GM's years-long failure to fully protect its vehicles from that attack doesn't reflect on GM's negligence, so much as a lack of security preparation in the entire industry of Internet-connected cars.**

---

"We basically had complete control of the car except the steering," says Karl Koscher, one of the security researchers who helped to develop the attack. "Certainly it would have been better if it had been patched sooner."

But the researchers argue that GM's years-long failure to fully protect its vehicles from

that attack doesn't reflect on GM's negligence, so much as a lack of security preparation in the entire industry of Internet-connected cars. Automakers five years ago simply weren't equipped to fix hackable bugs in their vehicles' software, the way that Microsoft and Google have long fixed bugs within weeks or even hours after they are disclosed to them. And many of those companies may not be much better prepared today.

"They just didn't have the capabilities we take for granted in the desktop and server world," says Stefan Savage, the UCSD professor who led one of the two university teams who

worked together to hack the Impala. “It’s kind of sad that the whole industry was not in a place to deal with this at the time, and that today, five years later, there still isn’t a universal incident response and update system that exists.”

In fact, GM tells WIRED that it has since developed the ability to push so-called “over-the-air” updates to its vehicles. The company eventually used that technique to patch the software in its OnStar computers via the same cellular Internet connection the UCSD and UW researchers exploited to hack the Impala. Starting in November of 2014, through the first months of 2015, the company says it silently pushed out a software update over its Verizon network to millions of vehicle with the vulnerable Generation 8 OnStar computer.



Security researcher Karl Koscher (L) at DEFCON. RYAN YOUNG FOR WIRED

Aside from the strangely delayed timing of that patch, even the existence of any cellular update feature comes as a surprise to the UCSD and UW researchers. They had believed that the OnStar computers could be patched only by driving them one-by-one to a dealership, a cumbersome and expensive fix that would have likely required a recall.

GM chief product cybersecurity officer Jeff Massimilla hints to WIRED that performing the cellular update on five-year-old OnStar computers required some sort of clever hack, though he refused to share details. “We provided a software update over the air that allowed us to remediate the vulnerability,” Massimilla writes in an email. “We were able to find a way to deliver over-the-air updates on a system that was not necessarily designed to do so.”

But Massimilla also admits that GM took so long to fully protect its vehicles because it simply wasn't ready in 2010 to deal with the threat of car hackers. He contrasts that response to GM's cybersecurity practices today, such as issuing a fix in just two days when it was alerted to a flaw in its iOS OnStar app in July. "The auto industry as a whole, like many other industries, is focused on applying the appropriate emphasis on cybersecurity," he writes. "Five years ago, the organization was not structured optimally to fully address the concern. Today, that's no longer the case."

### A Brilliant Hack Lullaby Ahead of Its Time

GM's glacial response is partly a result of just how far ahead of its time the UCSD and UW researchers' OnStar attack was. Their technique, described in a pair of papers in 2010 and 2011, represented a brilliant and unprecedented chain of hacker attacks integrated into a single exploit.

The intrusion technique began with a phone call to the Impala's OnStar computer. Because Verizon's voice network coverage was more reliable than its data network, the OnStar computers were programmed to establish a connection to any computer that played a certain series of audio tones, like an old-fashioned modem. UW's Koscher reverse engineered that audio protocol and created an mp3 file that could trigger a vulnerability in the computer known as a "buffer overflow."

---

**Put simply, "you play this song to it, and the car's taken over," says UCSD's Savage.**

---

From that initial audio attack, the attackers could pivot to take control of the OnStar computer's higher-bandwidth data connection and finally penetrate the car's CAN bus, the collection of networked computers

inside a vehicle that control everything from its windshield wipers to its brakes and transmission. Put simply, "you play this song to it, and the car's taken over," says UCSD's Savage.

### How GM Tried (And Failed) to Fix It: A Timeline

GM did, in fact, make real efforts between 2010 and late 2014 to shield its vehicles from that attack method, and patched the flaws it used in later versions of OnStar. But until the

surreptitious over-the-air patch it finished rolling out this year, none of its security measures fully prevented the exploit in vehicles using the vulnerable eighth generation OnStar units. Given that GM told the FCC it had two million Generation 9 Onstar computers deployed in 2011, former UCSD researcher Stephen Checkoway estimates that it had sold at least that many Generation 8 OnStar-enabled vehicles, too. “I would expect there were still several million vulnerable vehicles on the road,” Checkoway says.

Instead of updating the software on those Generation 8 OnStar units, GM first tried to block the attack on its cellular network. Sometime in 2011, it had Verizon put in a place a new measure on its wireless network to block data connections from OnStar computers to any server other than those approved as those belonging to GM.



But the researchers quickly found that a flaw existed in that fix, too. One in every 10 or 12 times that they restarted their Impala, its OnStar registered with the Verizon network in a way that somehow failed to prevent it from connecting to a malicious server, allowing their exploit to work again; An attacker could have auto-dialed thousands of phone numbers to find and hack the fraction of vehicles in that unsafe mode. Even the researchers say they never fully understood why the Verizon network protection measure failed, though they say they warned GM about the problem within a few months of finding it.

GM claims that it responded by tweaking its network protection again, but even those secondary measures seem to have failed. In 2012, the researchers were able to demonstrate their Impala hack for a [PBS Nova documentary](#) despite Verizon’s and GM’s attempts to block it. In late 2014, they demonstrated it yet again for a [60 Minutes episode](#) that would air in February of 2015. (For both shows they carefully masking-taped the car’s logos to prevent it from being identified, though [car blog Jalopnik nonetheless identified the Impala](#) from the *60 Minutes* demo.)

Here’s Koscher demonstrating the exploit on *60 Minutes* earlier this year:



car hacked on 60 minutes



### The Case For Publicly Disclosing Hacks?

GM's long-running failure to fully protect its vehicles from the OnStar exploit, compared with Chrysler's immediate patch and recall in July, could be interpreted as a lesson for hackers who keep their attacks secret rather than release them to motivate companies to quickly patch software. Chrysler was pressured into its response in part because hackers Charlie Miller and Chris Valasek staged a [flashy demonstration](#) for WIRED, named their target Jeep's make and model, and even published some portion of their code. "One of the reasons we chose the route we chose—this big to-do—is the takeaway we'd gotten from the academics' work," says Miller. "It didn't have the impact we wanted to have."

But UCSD professor Savage argues that publicly releasing details of the OnStar hack in 2010 might have done more harm than good. Even if key elements had been hidden, any publicity could have still enabled malicious hackers to rebuild the attack at a time when GM was unprepared to protect drivers from it. "This was so damn new to everybody: the regulators, the industry, the suppliers," he says. "Just figuring out how to wrap their heads around it was a significant undertaking."

Savage also notes that he's seen no evidence that the attack was discovered by any hackers in the five years that it remained secretly viable. He admits, however, that it could have been stealthily exploited by sophisticated state-sponsored hackers. Savage says his team briefed a wide variety of government and even military agencies about their work—those interested in "both defense and offense," he says—though they were careful not to disclose the Impala's make or model even in those private meetings.





Still, Savage says that if he were doing the same research today, he'd reconsider the decision to shield GM from public pressure. When he, Koscher, and other researchers revealed another car hacking technique in August, for instance—this time hijacking cars through a common Internet-connected gadget many drivers plug into their dashboards for insurance purposes—they publicly named every company whose bugs they'd exploited.

That shift to full-disclosure mode, Savage says, comes from watching car companies over the last five years as they've become aware of the possibilities of car hacking—partly thanks to UCSD and UW's research. Today, publishing car hacking techniques may be a powerful method to force companies to take responsibility for their vehicles' security.


In other words, automakers shouldn't expect him or any other researcher to keep their bugs hidden for five years again. "If I was to find a new one of these exploits today, I might make different choices," he says. "For companies now, protecting cars is more a question of resources and will. But not ignorance."

#CAR HACKING #CHRYSLER #GM #INTERNET-CONNECTED CARS


VIEW COMMENTS

## SPONSORED STORIES


POWERED BY OUTBRAIN




KELLEY BLUE BOOK  
2015's Top 10 Best Car Buys




ELIO MOTORS  
The Anti-Tesla: The Elio Is Low-Cost, High-Mileage, and Very




THE SOVEREIGN IN VESTOR  
\$5 Bill Proves The Economy Is About To Collapse



MINT  
Your 401(k) Isn't Growing as Fast as It Should - Here's Why



UNLIMITED REVS  
10 Cars You Don't Want To Own




COMPARE.COM  
The American People Have Been Trained and Mislead into

WE RECOMMEND

http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/

Page 7 of 9






WIRED OPINION

Hey FCC, Don't Lock Down Our Wi-Fi Routers

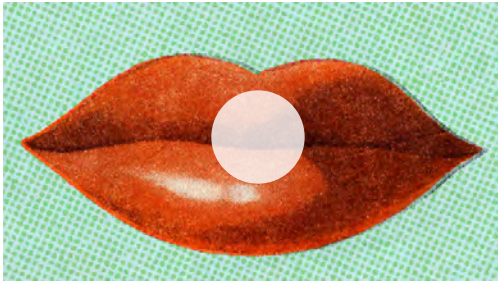
6 HOURS



ANALYSIS

Google's Three Tips for Sabotaging the Cybercrime Economy

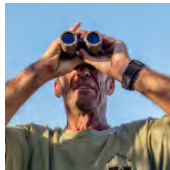
24 HOURS



EXPLAINED

Answers to Your Burning Questions on the Ashley Madison Hack

08.21.15



PHOTOGRAPHY


On a Mission With the Men of Arizona Border Recon

2 DAYS

HACK BRIEF


HACK BRIEF: MOBILE MANAGER'S SECURITY HOLE WOULD LET HACKERS WIPE PHONES

09.22.15




WIRED INSIDER

An Un-stealable Bike Has Arrived




DAVID PIERCE

Hands-On With the Huge New Apple iPad Pro and Pencil Stylus




NICK STOCKTON

2,500 Tons of Rock Fell Off Half Dome and Nobody Noticed



LIZ STINSON


This Bridge Goes Nowhere, and That's Just Fine by Us



KELLEY BLUE BOOK

The 10 Best 3-Row Vehicles

POWERED BY OUTBRAIN




ARE YOUR OFFICE PHONES BUILT FOR BUSINESS?

COMCAST BUSINESS B4B

Find voice solutions for companies of all sizes

GET THE MAGAZINE

Subscribe now to get 6 months for \$5 - plus a FREE Portable Phone Charger.



SUBSCRIBE

GET OUR NEWSLETTER

WIRED's biggest stories, delivered to your inbox.

Enter your email

SUBMIT

FOLLOW US ON FACEBOOK

Don't miss our latest news, features and

FOLLOW

http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/

Page 8 of 9

[SUBSCRIBE](#) | [ADVERTISE](#) | [SITE MAP](#) | [PRESS CENTER](#) | [FAQ](#) | [CUSTOMER CARE](#) | [CONTACT US](#) | [NEWSLETTER](#) | [WIRED STAFF](#) | [JOBS](#) | [RSS](#)

Use of this site constitutes acceptance of our [user agreement](#) (effective 3/21/12) and [privacy policy](#) (effective 3/21/12). [Your California privacy rights](#).  
The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written [permission of Condé Nast](#).

---